Escalatieprotocol afsluiten SUWInet

In dit protocol wordt beschreven uit welke stappen het "escalatieprotocol afsluiten SUWInet" bestaat. Iedere stap in het protocol is erop gericht om te bewerkstelligen dat tekortkomingen in de beveiliging van SUWInet worden weggenomen. Als ultimum remedium is het mogelijk om een gemeente af te sluiten van het gebruik van SUWInet. Afsluiting van het gebruik van SUWInet heeft vergaande consequenties voor de burger. Hij/zij moet zijn/haar gegevens opnieuw aanleveren en wordt daarmee onevenredig belast.

STAP 1 Zelfevaluatie (vrijwillig)
Gemeenten kunnen via een zelftest van de VNG onderzoeken of wordt voldaan aan de normen uit het SUWI-normenkader. De zelftest is een analyse die aangeeft op welke onderdelen uit het SUWI-normenkader aanpassingen of verbeteringen aangebracht moeten worden. De zelftest is daarmee een instrument van en voor gemeenten *zelf* om invulling te geven aan de verantwoordelijkheid voor de beveiliging van de gegevens die via SUWInet worden ontvangen. Het verdient aanbeveling om de uitkomsten van de zelftest in het College van B&W te agenderen en het (eventuele) verbeterplan dat daaruit volgt door het College van B&W te laten vaststellen en hierover de gemeenteraad te informeren. Maatregelen kunnen ook worden opgenomen in het jaarlijks verplicht op te stellen beveiligingsplan en/of het verslag over de verantwoording.

STAP 2 Jaarverslag (bestaande wettelijke verplichting)
Op grond van de SUWI wet-en regelgeving[1] is geregeld dat iedere gebruiker van Suwinet, dat wil zeggen het UWV, de SVB en de colleges van B&W voor de SUWI-taken aantoont dat het stelsel van de door zijn organisatie genomen maatregelen voldoet aan het SUWI-normenkader. Het jaarlijkse verslag over het gebruik van SUWInet moet ieder jaar worden vastgesteld. Het aantonen gebeurt door in te gaan op opzet, bestaan, werking en controleerbaarheid van het stelsel van maatregelen en procedures gericht op de gegevenshuishouding in relatie tot SUWInet. De rapportage dient te worden bevestigd met een oordeel (van getrouwheid) van een tot de Nederlandse Orde van Register EDP-Auditor toegelaten persoon. De verantwoording over de informatiebeveiliging biedt het college van B&W en de gemeenteraad een handvat om hun verantwoordelijkheid voor informatiebeveiliging en bescherming van persoonsgegevens in te vullen. Daarnaast kunnen burgers er vertrouwen aan ontlenen dat gemeenten de aan hen toevertrouwde gegevens zorgvuldig verwerken.

STAP 3 Onderzoek van de Inspectie SZW
De Inspectie SZW houdt toezicht op de wijze waarop het UWV, de SVB, en de colleges van burgemeester en wethouders bij de uitvoering van de aan hen opgedragen taken samenwerken. Het toezicht van de inspectie is onafhankelijk en signalerend. De aard en intensiteit van het toezicht hangen af van de kwaliteit van de uitvoering en de risico's die zich in de uitvoering voordoen. De risico's betreffende de informatiebeveiliging van SUWInet bij gemeenten wordt betrokken bij het opstellen van het jaarplan van de Inspectie. De mate waarin gemeenten hebben aangetoond dat de beveiliging van SUWInet op orde is, zal leidend zijn voor de intensiteit van onderzoek door de inspectie. Onderzoeken van de Inspectie SZW naar de beveiliging van SUWInet richten zich op de 7 normen uit het SUWI-normenkader. Uit het onderzoek van de Inspectie SZW volgt welke gemeenten niet aan alle 7 (essentiële) normen voldoen. Voor gemeenten die niet voldoen aan de 7 essentiële normen treedt stap 4 in werking. Het College Bescherming Persoonsgegevens zal worden geïnformeerd over de resultaten van het onderzoek van de Inspectie SZW.

STAP 4 Aankondiging tot een aanwijzing
De gemeente die niet aan alle 7 essentiële normen voldoet ontvangt een aankondiging tot een aanwijzing. De gemeente ontvangt dan een brief waarin het voornemen tot een aanwijzing wordt aangekondigd. De gemeente krijgt in deze fase een laatste mogelijkheid om de beveiliging van

[1] Artikel 5.22 besluit SUWI en artikel 5.22 en 6.4 van de Regeling SUWI.

SUWInet op orde te brengen. In deze aankondiging zal een termijn worden genoemd, die afhankelijk is van de specifieke situatie in de betreffende gemeente. Na de genoemde termijn zal de gemeente moeten aangeven of de onrechtmatige situatie is hersteld en wordt voldaan aan alle 7 essentiële normen. Afhankelijk van de situatie kan het voorkomen dat een gemeente nog niet aan 1 norm kan voldoen. Met deze gemeente worden nadere afspraken gemaakt over de termijn waarbinnen alsnog aan deze norm wordt voldaan.

STAP 5 Aanwijzing tot het op orde brengen van de beveiliging van SUWInet
Een gemeente die geen verantwoordelijkheid neemt voor de beveiliging van SUWInet en ook na de aankondiging van de aanwijzing geen orde op zaken heeft gesteld, zal een aanwijzing ontvangen. Een mogelijke aanwijzing kan zijn dat een gemeente wordt verplicht om, na een daartoe door SZW gestelde termijn, door middel van een audit aan te tonen dat de beveiliging van SUWInet op orde is. Dit is een relatieve milde aanwijzing. Dit kan aan de orde zijn als de gemeente verbeteringen heeft doorgevoerd, maar nog een aantal punten niet heeft opgelost. Ook kan een aanwijzing worden gegeven waarin de gemeente wordt opgedragen om een externe deskundige in te huren om de beveiliging van SUWInet op orde te brengen. De Minister van SZW bepaalt aan welke voorwaarden de externe deskundige dient te voldoen en welk resultaat bereikt dient te worden, voordat de gemeente weer zelfstandig de uitvoering ter hand kan nemen. De kosten voor het uitvoeren van een audit of het inhuren van één of meerdere externe deskundigen zijn volledig voor rekening van de gemeente. Dit zal aan de orde zijn als de gemeente er blijk van heeft gegeven het herstellen van de onrechtmatigheden niet zelfstandig uit te kunnen voeren.

STAP 6 Treffen van noodzakelijke voorziening tot het afsluiten van SUWInet
Indien een gemeente zelfs de aanwijzing niet opvolgt, zal de Minister van SZW zelf in de zaak voorzien. Zo kan de Minister zelf een externe deskundige aanstellen en bij een gemeente installeren, uiteraard op kosten van die gemeente.[2] In situaties waarin er een acuut en reëel risico is op grove schendingen van de privacy van burgers, kan het geboden zijn een gemeente (tijdelijk) van SUWInet af te sluiten. De minister van SZW zal op dat moment aan de beheerder vragen om de verleende autorisaties voor SUWInet in te trekken. Dit betekent dat er geen mogelijkheid meer is voor gemeenten om gegevens in te zien. Gemeenten zullen wel gegevens kunnen blijven leveren. Het afsluiten van SUWInet heeft tot gevolg dat gemeenten zelf informatie van hun burgers zullen moeten vragen, of via individuele overeenkomsten met andere partners in de keten moeten betrekken. Voor zover die partners op grond van staande wetgeving niet zijn gehouden deze gegevens kosteloos te verstrekken, kunnen ook hiervoor kosten in rekening worden gebracht.

Toezicht College Bescherming Persoonsgegevens
De minister kan op ieder moment in het proces of wanneer daartoe aanleiding is het College Bescherming Persoonsgegevens informeren en vragen om handhavend op te treden. Het College Bescherming Persoonsgegevens maakt vervolgens een zelfstandige afweging of het overgaat tot het verrichten van een onderzoek.

Het CBP kan een last onder dwangsom opleggen indien uit onderzoek van het CBP blijkt dat gemeenten niet voldoen aan de Wet bescherming persoonsgegevens. Een andere mogelijkheid is het opleggen van een boete. De wet die regelt dat het College Bescherming Persoonsgegevens (CBP) de bevoegdheid heeft om aan verantwoordelijken en bewerkers bestuurlijke boetes op te leggen voor overtredingen van de Wet bescherming persoonsgegevens (Wbp) en andere specifieke dataprotectieregels is door de Eerste Kamer aanvaard en zal vermoedelijk op 1 januari 2016 in werking treden. De boete kan maximaal € 810.000 bedragen.

[2] Gedacht kan worden aan bijvoorbeeld inhuur vanuit ABD-topconsult.